2008/2009 : Report 4

OFFICE OF THE

Auditor General of British Columbia

Managing Government's Payment Processing

May 2008

2008/2009 : Report 4

OFFICE OF THE

Auditor General of British Columbia

Managing Government's Payment Processing

May 2008

Library and Archives Canada Cataloguing in Publication Data

British Columbia. Office of the Auditor General.

Managing government's payment processing

(Report ; 2008/2009: 4)

ISBN 978-0-7726-5986-6

1. Finance, Public - British Columbia - Accounting -Data processing - Evaluation. 2. Administrative agencies - British Columbia - Accounting - Data processing - Evaluation. I. Title. II. Series: British Columbia. Office of the Auditor General. Report ; 2008/2009: 4.

HJ9921.Z9.B74 2008 352.4'309711 C2008-960091-6

OFFICE OF THE
Auditor General
of British Columbia

LOCATION:
8 Bastion Square
Victoria, British Columbia
V8V 1X4

OFFICE HOURS:
Monday to Friday
8:30 a.m. – 4:30 p.m.

TELEPHONE:
250 387-6803
Toll free through Enquiry BC at: 1 800 663-7867
In Vancouver dial 660-2421

FAX: 250 387-1230

E-MAIL: bcauditor@bcauditor.com

WEBSITE:
This report and others are available at our Website, which also contains further information about the Office: www.bcauditor.com

REPRODUCING:
Information presented here is the intellectual property of the Auditor General of British Columbia and is copyright protected in right of the Crown. We invite readers to reproduce any material, asking only that they credit our Office with authorship when any information, results or recommendations are used.

OFFICE OF THE
Auditor General
of British Columbia

8 Bastion Square
Victoria, British Columbia
Canada V8V 1X4
Telephone: 250 387-6803
Facsimile: 250 387-1230
Website: http://bcauditor.com

The Honourable Bill Barisoff
Speaker of the Legislative Assembly
Province of British Columbia
Parliament Buildings
Victoria, British Columbia
V8V 1X4

Dear Sir:

I have the honour to transmit herewith to the Legislative Assembly of British Columbia my 2008/2009 Report 4: Managing Government's Payment Processing.

John Doyle, MBA, CA
Auditor General of British Columbia

Victoria, British Columbia
May 2008

copy: Mr. E. George MacMinn, Q.C.
Clerk of the Legislative Assembly

Table of Contents

Auditor General's Comments 1

Executive Summary 3

Overall Conclusion 5

Key Findings 6

Our Key Recommendations 6

Response by Government 9

Detailed Report 11

How payments are handled 13

What could go wrong? 14

Audit Purpose and Scope 14

A. Administration and maintenance of access 18

B. Generation of payment and bank reconciliation files and transfer to MVS for further processing 21

C. Processing and release of EFT payments 25

D. Processing and printing cheques 27

E. Management of the status of payments 29

F. Reconciliation of payments to the general ledger 31

G. Back-up of program and payment files 33

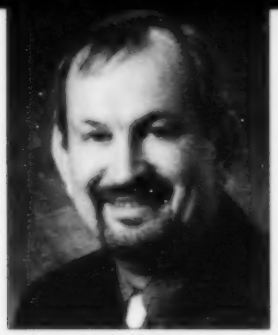
H. Business continuity planning 35

Appendices 39

A. Glossary 41

B. Office of the Auditor General Reports Issued During Fiscal 2008/2009 45

Auditor General's Comments



John Doyle
Auditor General

Each year, government makes millions of payments, totalling tens of billions of dollars, to many thousands of suppliers and employees. The public expects that these payments should be sent to the right parties, in the right amounts, and in a timely way. It's also expected that government should have adequate controls to ensure that none of the payments go missing along the way, through error or fraud.

Although in today's world of computerized processing, many of the key controls are built into the system, or the proverbial 'black box', complementary manual controls are also needed to ensure a robust control environment.

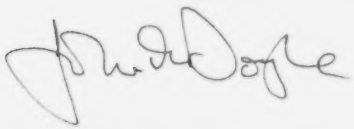
This audit is part of the ongoing review we have been carrying out on government's key financial systems. In two prior audits we published on the corporate accounting system, we examined the controls in place over the operating system, database and key components of the Oracle financial application. We stopped short, however, of looking at what happens after the approved payment information is sent for processing. This audit completes the end-to-end review by examining automated and manual controls over the processing and management of both electronically transferred and cheque-based payments.

In most respects, the controls were found to be operating as expected. However, we found some shortcomings, which I have brought to government's attention, so controls can be further strengthened.

Information technology is pervasive in our society. It is also used extensively throughout government to help it deliver its programs and services. Since well-designed and effective use of information technologies is a critical success factor for government, I intend to increase the future focus of my office to examine technology related issues.

Auditor General's Comments

I would like to thank the staff in the Ministry of Finance and Ministry of Labour and Citizens' Services for the cooperation and assistance they provided to my staff during their work on this audit.



John Doyle, MBA, CA
Auditor General of British Columbia

Victoria, British Columbia
May 2008

Audit Team

Bill Gilhooly, Assistant Auditor General

Faye Fletcher, IT Audit Specialist

David Lau, IT Audit Specialist

Joji Fortin, Manager

Rob Cowley, IT Audit Analyst

Executive Summary

Government processes millions of banking transactions—both electronic funds transfers and cheque payments—annually. Last year these transactions totaled over $30 billion. The volume of transactions processed can be shown by the following summary:

- Every day, an average 10,200 EFT transactions are processed for supplier payments, debt management/loan administration transfers, and grant payments.[1]
- Twice a month, medical services payments are processed, with an average 8,300 EFT transactions made per run.[1]
- Every two weeks, EFT transactions are transmitted to the Credit Union Central of British Columbia for employee payroll. Approximately 30,000 employees are paid by direct deposit.[2]
- Every year, over 900,000 cheque payments are processed.[3]

Government relies on information technology (IT) to process this large volume of payments accurately, completely and on a timely basis. If EFT and cheque payment controls are not adequately designed and effective, processing errors and fraudulent activities could result in substantial financial loss.

Overall Conclusion

Overall, adequate controls are in place to manage risks associated with government's payment processing. We did, however, identify areas where controls, like providing access only on a "need to have" basis and monitoring for unusual activities, need to be improved to guard against financial losses. We also noted some key manual controls that have been designed to detect errors and potential fraudulent activities are in place, and therefore compensate for some control weaknesses identified.

---

1 Source – Based on EFT statistics maintained by Banking and Cash Management for period April 1, 2007 to February 29, 2008.

2 Source – Statistics from government's payroll services provided by TELUS Sourcing Solutions Inc.

3 Source – Bank Billing System report for the period January 1 to December 31, 2007, provided by Banking and Cash Management Branch.

Executive Summary

Key Findings

- Most controls are automated and are operating as intended. Some manual controls, however, need improvement. Examples include the management review of key system-generated reports and of audit trails of system access, as well as some approvals for manual transactions.
- Some staff in several business process areas have too much access to computer programs and payment transactions. The risks this poses are further increased because monitoring controls are inadequate. In a few cases, access rights are also incompatible with job functions.
- Segregation is inadequate in several business areas between those administering and monitoring security and those handling daily production activities, and between those maintaining daily system production and those developing and testing changes to production programs. This poses risks of intentional and unintentional actions going undetected.
- Policies and procedures in some business areas are not up to date, and may provide inadequate guidance to staff.

Our Key Recommendations

This report is the result of our audit of controls in six separate business areas—generation of payment and control information, printing and distribution of cheque payments, processing and release of EFT payments, management of the status of payments, bank reconciliation processes, and back-up and business continuity planning.

We communicated our findings during our audit. In late 2007 and early 2008, we provided management with a detailed report on each of the six business areas we examined. We have not published all the detailed findings from these reports, in part to avoid introducing any security risks.

Exhibit 1 shows the number of recommendations we made by business area examined. We made 85 recommendations in total. Management has indicated that many have been, or are in the process of, being addressed. We will monitor progress and carry out a future follow-up.

In this report, we summarize only the key recommendations at the end of each section. Overall, these recommendations can be grouped into five themes:

- **Increase management review** — Management should increase regular reviews of key system-generated reports and transaction and access audit reports.
- **Remove inappropriate access** — Inappropriate access levels should be removed and access should be regularly reviewed to make sure individual access is compatible with the user's responsibilities.
- **Strengthen segregation of duties** — To minimize risks arising from the lack of appropriate segregation of duties, user activities should be evaluated and reassigned where necessary.
- **Step-up user monitoring activities** — Access activity reports should be regularly reviewed, especially for support staff with advanced access to programs and data and for updates to high-risk data and program files.
- **Keep policies and procedures current** — Policies and procedures should be updated to ensure guidance given staff remains current.

Exhibit 1:

Key Business Areas Audited and Total Detailed Recommendations Made

Audit Scope and Key Business Area	Number of Detailed Recommendations
A. Administration and maintenance of access to programs and data files	Included in report sections B to F
B. Generation of payment and bank reconciliation files from the corporate accounting system and ministry systems and transfer from UNIX to the MVS environment via file transfer protocol	21
C. Processing of electronic funds transfer payment transactions by Banking and Cash Management Branch's automated funds transfer system and release to financial institutions	15
D. Processing cheque payment transactions for printing at BC Mail Plus and mailing to payees	15
E. Management of the status of payments	15
F. Reconciliation of cheque and electronic funds transfer payments to those processed and authorized by the corporate accounting system	15
G. Regular back-up of program and payment files	0
H. Development, maintenance and regular testing of a business continuity plan	4
Total recommendations	**85**

Response by government

The following is a combined response from Provincial Treasury, Banking Cash Management and Information Systems branches, Ministry of Finance; and BC Mail Plus and Corporate Accounting Services branches within Common Business Services, Ministry of Labour and Citizens' Services.

We would like to express our appreciation to the audit team for their professionalism, attention to detail and commitment to obtaining a thorough understanding of the complex systems and controls involved in processing government's payments.

We are pleased and reassured by their conclusion that "adequate controls are in place to manage risks associated with government's payment processing". We are addressing recommendations on further enhancements in the areas of management monitoring and review, access, segregation of duties and documentation in three ways.

The first is the implementation of improvements completed during the course of audit field work. Examples include:

- Provincial Treasury: The consistent use of tick marks and initials to provide evidence that the matching of ministry payment information to the bank summary is, in fact, carried out each day.
- BC Mail Plus: All access for print operators and system analysts has been reviewed and updated where needed. In addition, the number of reviews performed on key system-generated reports, transactions and audit reports has been increased.

The second is the inclusion of recommendations into existing project initiatives. For example:

- Provincial Treasury: The ongoing payment procedure consolidation project will incorporate process improvements such as attaching a duplicate copy of the bank deposit slip for unclaimed cheque deposits to the summary report of unclaimed cheques to provide evidence that the deposit is complete.
- BC Mail Plus: The Cheque Printing and Procedures manual initiative will incorporate applicable audit recommendations.

- The joint Business Continuity Plan identified in our tri-partite Memorandum of Understanding will address the recommendations regarding business continuity and disaster recovery planning to ensure critical payments continue in the event of a disaster. The plan will include testing from our existing alternate disaster recovery sites.

Finally, we will undertake broader reviews based on the key audit recommendations to assess the remaining recommendations from the detailed management reports.

Provincial Treasury is undertaking an information systems security review to be completed by the end of June 2008, identifying action items that will form the basis of enhancement project initiatives for the upcoming business cycles.

Corporate Accounting Services, Common Business Services, Ministry of Labour and Citizens' Services is in the process of developing a detailed plan to address all recommendations. A review of security, access audit procedures and logs, and segregation of duties is already underway with changes implemented to further enhance access and audit data. Further, a full review of the file transfer protocols will be undertaken and procedural manuals will be updated to reflect change management processes.

In conclusion, we generally agree with the key findings and recommendations of the Auditor General's report and are committed to implementing a three phased strategy to strengthen Government's payment processing controls.

Detailed Report

How payments are handled

Several business areas work together to manage and process government payments in the following steps:

- Corporate Accounting Services, in the Ministry of Labour and Citizens' Services, generates data files for the control and production of both cheques and electronic funds transfer (EFT) transactions.
- Corporate Accounting Services provides a daily payment print file to BC Mail Plus (part of the same ministry) for cheque printing and mailing, and an EFT file to the Banking and Cash Management Branch in the Ministry of Finance.
- The Banking and Cash Management Branch releases the EFT file to a financial institution for distribution and direct depositing to payee accounts. It also provides management services on the status of government issued payments (e.g., payments stopped by government, cheques returned and EFTs rejected by the bank).
- In addition to generating payment files, Corporate Accounting Services also performs daily and monthly bank reconciliations.

Managing and processing government's payments requires an adequate control structure both to ensure that only authorized cheque and EFT transactions are paid; and to ensure that outstanding cheques and EFTs reflect valid payments.

The use of EFTs is generally considered to be fast, secure, low cost and low risk for suppliers. There is valuable time savings for payees, who need not go to the bank to deposit a cheque.

There are also benefits to government, with EFTs offering:

- lower cash and cheque-handling costs than are associated with paper cheques;
- reduced use of paper;
- elimination of the risk of paper cheques being lost or stolen in the mail;
- more timely supplier payments and faster access to funds (many banks credit direct deposits faster than paper cheques); and
- easier reconciliation of payments to bank statements.

Detailed Report

What could go wrong?

As in any payment processing system, government must manage a number of risks in processing its EFT and cheque payments. These include the risk of loss due to clerical errors, the risk of hardware and software failures, and the risk that someone will intentionally alter a payment transaction to misdirect or misappropriate funds.

There are other risks, too. Just as paper cheques may sometimes be stopped because of errors in payment details, EFT payments may also be rejected and returned by the bank because of invalid bank account information. Government, too, may recall a payment if it turns out that the payee is not entitled to it (e.g., for an overpayment or a duplicate payment) or that, in the case of payroll, the payee has been terminated or is deceased. Cheques may also be undeliverable or unclaimed. All of these circumstances create a risk of missing or late payments, or of returned or recalled items not being promptly handled. There is a further risk that government could incur a loss if stop payments are not dealt with immediately.

Audit Purpose and Scope

Purpose of Audit

The purpose of this audit was to evaluate the automated and manual business controls designed to support control objectives of completeness, accuracy, validity and timeliness of government's EFT and cheque payments. Not only must *EFT processes* have highly efficient controls built into the systems, but the processes must be controlled at the sender and recipient sides. As well, controls must exist at the intermediary stages wherever information is passed, stored and processed. *Cheque management processes* also require an adequate control structure to ensure that only authorized cheques are paid by the bank and that all outstanding cheques reflect only valid payments and are not duplicated.

This report provides an assessment of the adequacy of controls in place at each stage of the EFT and cheque management processes.

Detailed Report

Scope

We examined the key processes involved in the required processing and transfer of payment information at the following stages, resulting in the production and distribution of cheque and EFT payments:

> Corporate Accounting Services ➔ MVS environment via file transfer protocol (FTP) ➔ BC Mail Plus on MVS ➔ Banking and Cash Management Branch on MVS and to financial institutions.

We also reviewed the bank reconciliation processes carried out by Corporate Accounting Services to ensure that all authorized payments are being processed accurately, completely and on a timely basis and that no other payments have been made.

Exhibit 2 on page 17 provides an overview of the key business areas and cheque and EFT payment processes we examined.

This required us to assess controls related to the cheque-printing system (advanced function printing [AFP]), the cheque management system (CHQ), the automated fund transfer system (AFT), and the bank reconciliation system (BRS). These four systems run in government's MVS mainframe operating environment.[1]

We carried out the audit from June 2007 to February 2008.

Audit Criteria

Our audit was based on criteria set out in the *Information Technology Control Guidelines* issued by the Canadian Institute of Chartered Accountants. We used the standard control objectives provided in these guidelines to assess the design and the effectiveness of the IT controls in place.

We conducted the audit in accordance with the assurance standards recommended by the Canadian Institute of Chartered Accountants. Accordingly, it included tests and other procedures we considered necessary to obtain sufficient and appropriate evidence to support our conclusions.

[1] The MVS system, maintained by TELUS in Victoria, was upgraded to the latest level of z/OS (often referred to as MVS) on January 14, 2007. The security software used in this mainframe environment is called Resource Access Control Facility (RACF).

We focused on evaluating system-based and manual controls in the following business processes:

A. Administration and maintenance of access to computer programs and data files

B. Generation of payment and bank reconciliation files based on transactions from CAS and ministry systems; the transfer of the payment files from UNIX to the MVS environment; and the creation of separate files containing EFT and cheque payment transactions, control totals and payee statements

C. Processing of EFT payment transactions by Banking and Cash Management's automated fund transfer (AFT) system and the release of the payments to financial institutions

D. Processing of cheque payment transactions so cheques can be printed at BC Mail Plus and then distributed to suppliers

E. Management of the status of payments (including the identification of cleared, outstanding and rejected cheque and EFT payments), and of the process for dealing with fraudulent, altered and unclaimed cheques

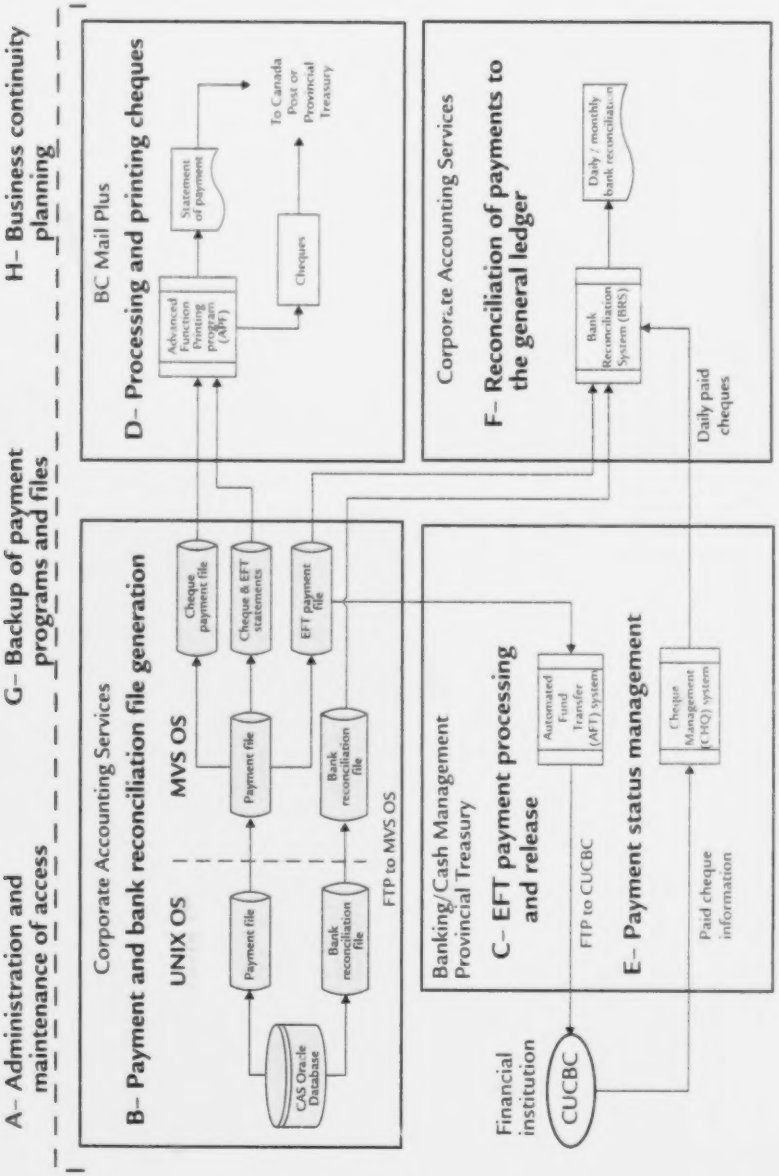
F. Reconciliation of cheque and EFT payments to those processed and authorized by CAS

G. Regular back-up of payment files to ensure that payment processing can continue after a temporary disruption in operations

H. Development, maintenance and regular testing of a business continuity plan that allows critical payments to continue in the event of a disaster

Exhibit 2:

Overview of the Key Business Areas and Cheque and EFT Payments Processes Examined, as Indicated by A to H.



Source: Compiled by the Office of the Auditor General of British Columbia

A. Administration and maintenance of access

Administration and maintenance of access to computer programs and payment data files should be improved.

In our first report on the corporate accounting system[5], we examined the processes and practices used to govern a complex IT and business environment. Governance and administration over the processes in this audit are equally important, especially given the variety of stakeholders and government organizations involved in the payment process.

In this section of the audit, we looked at several control areas related to the administration and maintenance of access, including ownership of resources, data classification, data security and administration, and user access and monitoring.

Our focus was on payment transactions processed in the MVS environment. The software that provides security in this environment is called Resource Access Control Facility (RACF). It identifies and verifies users entering the system and restricts their capabilities and access to data and computer programs. It also allows the security administrator to log and report various security related activities.

For each organizational unit, a Government Data Security Administrator is responsible for controlling and managing resources — for example, userids, groups, data and program files. Banking and Cash Management, Corporate Accounting Services and BC Mail Plus each has its own such administrator.

We examined the controls in place at Banking and Cash Management, Corporate Accounting Services and BC Mail Plus, to address several key risks that would put the integrity and security of payment transactions in question. Those include the risk that:

- ownership of, and responsibility for, resources required to process EFT and cheque payments has not been clearly defined;
- inappropriate personnel have security administration capabilities that give them access to all data and programs;

[5] For copies of these reports, visit www.bcauditor.com

- users, including systems support, have access to computer programs and data files at a level beyond that required to perform their jobs; and
- inappropriate access to the programs and data is not detected.

Key Findings

- Government has developed data classification policies, standards and guidelines for managing payment data. Although management has not reviewed the information in mainframe environments to see where it fits into the revised government classification scheme, we have confirmed that every key computer program and data file has a RACF security profile associated with it that can limit access to appropriate levels.
- Standard procedures are followed for requesting the establishment of a new userid and access capabilities. A controlled process exists for distributing and controlling passwords.
- Although there are procedures to ensure users are connected to the right groups, staff access in some instances is not compatible with responsibilities and occasionally even exceeds job requirements.
- Segregation is inadequate in several business areas between those who are administering and monitoring security and those involved in daily production and maintenance activities. This does not follow best practices, as those responsible for security administration should have only "read access" to the production environment.
- Certain support staff have the ability to change production, test and development programs and data. This results in a lack of separation of duties between these functions and creates an environment where error or inappropriate activity could go undetected.
- High-risk activities, including changes to programs and data, are not always logged and later reviewed.

- The files containing records for activities that are logged at Corporate Accounting Services can be altered by those responsible for monitoring audit reports. This risk is further increased as these same staff support daily production operations.
- The responsibility for monitoring access activity reports is not clear between the Information Systems Branch in Provincial Treasury and the Information Management Branch in the Ministry of Finance. As a result, monitoring is not performed in all cases.

Key Recommendations

- User and group access should be regularly reviewed to ensure that it is consistent with operational duties and responsibilities and that proper segregation of duties is maintained.
- Risks associated with the lack of segregation between those administering and monitoring security and those handling daily production activities, and between those maintaining daily system production and those developing and testing changes to production programs should be evaluated. Possible consequences and mitigations should be considered, including whether any residual risks are acceptable.
- Security profiles protecting payment, bank reconciliation and computer program files should include logging all change activities for later review.
- Procedures should be established and carried out to regularly monitor and investigate, as required, activities where changes are made to high-risk data and programs.
- Access to audit logs should be granted only on a "need to have" basis.
- The relationship and responsibilities between the Provincial Treasury Information Systems Branch and the Ministry of Finance Information Management Branch should be more clearly documented and communicated.

B. Generation of payment and bank reconciliation files and transfer to MVS for further processing

Controls should be improved over the generation of payment and bank reconciliation files, their transfer from UNIX to MVS, and subsequent processing.

The process to generate and distribute government's EFT and cheque payments starts at Corporate Accounting Services when an authorized daily payment file is created from the government's corporate accounting system and other ministry systems. The initial payment extract file and bank reconciliation adjustment file are created in the UNIX operating environment. They are then transferred to the MVS operating environment, where separate files containing manual cheque and EFT payments and related statement and control information are produced. In this environment, payment and reconciliation information is made available to: BC Mail Plus (to print manual cheques); Banking and Cash Management (for subsequent release to the Credit Union Central of British Columbia [CUCBC—i.e., "the bank"] for EFT payments and management of payments); and Corporate Accounting Services (to perform bank reconciliations).

All of these processes happen inside the "black box,"[6] shown as section B in Exhibit 2.

In this section of the audit, we looked at the key processes involved in: the generation of payment files that are based on transactions from the corporate accounting system and other ministry feeder systems; the transfer of the payment and bank reconciliation files from UNIX to the MVS environment via file transfer protocol (FTP), and the creation of the EFT and cheque payment files and related statement and control information.

[6] The UNIX operating system is located at 4000 Seymour Place, Victoria, in a multi-purpose platform area. Workplace Technology Services (WTS), part of the Ministry of Labour and Citizens' Services, provides full support for the UNIX operating system. The MVS system, maintained by TELUS, is also located at 4000 Seymour Place, Victoria. The security software used in this mainframe environment is Resource Access Control Facility (RACF).

File transfer protocol (FTP) is a network protocol used to transfer data from one computer to another through a network, such as over the Internet.

We focused on the controls in place to address the risk that:

- payment transactions in files delivered to the MVS environment are incomplete, inaccurate or unauthorized, or are not delivered in a timely manner; and
- the files containing EFT and cheque payment transactions created in the MVS environment are incomplete, inaccurate or unauthorized, or are not delivered in a timely manner.

Generation of payment files in the UNIX environment

Key Findings

- A small group of staff are responsible for UNIX processing, making adequate segregation of duties difficult among programmers, testers and production staff.
- As soon as the payment file is created, it is automatically sent via FTP to the MVS environment. Once the payment file job finishes, the file is immediately backed up and deleted. This reduces the risk of either unintentional or fraudulent changes to payment information.
- The payment file exists for only a short period, however during that time, access to the file is not appropriately restricted to ensure confidentiality and integrity of the payment information.
- A large number of users have "root" access—that is, full access to the UNIX server and all directories, including log files. No activity monitoring is conducted as a possible compensating control.

Key Recommendations

- Management should review access to ensure proper segregation of duties between staff able to set up and run production processes and those responsible for development activities.
- Access to the payment file information should be further restricted to ensure its confidentiality and integrity.
- A review of "root" access relative to job descriptions and requirements should be performed, and management should formally approve "root" access in each case. Any excessive access should be removed.

- Management should investigate whether software could be used to delegate "root" user capabilities, and audit all activities with this authority.

Use of File Transfer Protocol to transfer payment files to MVS

File transfer protocol (FTP) is used throughout the payment processes for transferring payment and reconciliation data between processing environments. We examined the transfer of data from the UNIX environment to the MVS environment at government's mainframe processing facility.

To satisfy control requirements in other sections of our audit, we also examined the transfer of payment data from Banking and Cash Management to the CUCBC, and the transfer of paid cheque and returned cheque items from CUCBC to Banking and Cash Management. (See Exhibit 2)

Key Findings

- Secured FTP is used by Banking and Cash Management to transfer data to and from the CUCBC.
- The transfer of data by Corporate Accounting Services, between the UNIX and MVS operating environments, located within the same building, does not adequately protect the confidentiality of both logon credentials and data during transmission. Furthermore, controls are inadequate to ensure the transferred data is complete or accurate.
- Technical staff are electronically paged when the process completes successfully or if the process fails.

Key Recommendations

- Management should implement a more secure means of transferring files from UNIX to the mainframe environment. The method used should protect the confidentiality of logon credentials and data during transmission over the network.
- An audit trail of transaction counts and control totals should be implemented and checked on each file transmission. This would verify that information was not altered during the FTP process.

Creation of EFT and cheque payment files and control files in the MVS environment

Once the two files—payment transactions and bank reconciliation adjustments—are received in the MVS environment, the payment transactions are processed to divide the transactions into separate types of files. The files created (EFT payments, cheque payments, EFT statements, cheque statements, EFT control information, cheque control information and bank reconciliation information) are further processed and then relevant files are made available to BC Mail Plus, Banking and Cash Management, and Corporate Accounting Services. All processing after that relies on the integrity of these files.

Key Findings

- A small group is responsible for MVS processing, making adequate segregation of duties difficult. This has been noted in Section A of our report.
- A scheduled job runs every night. If a processing problem occurs, CAS Service Operations is notified and corrective action is taken to ensure processing is completed on time.
- Access to many payment, bank reconciliation and program files is not logged, except for failed attempts to "read" files. This has been noted in Section A of our report.
- The log used to record changes to programs is manual. There is no assurance that it is complete or accurate.

Key Recommendations

- To provide assurance on the completeness of the manual change log, high-level profiles protecting computer program files should be flagged, so that when a change is made, the user is identified and logged for later review.

C. Processing and release of EFT payments

Controls should be improved over processing EFT payment transactions and their release to financial institutions.

The majority of government payments are made through electronic funds transfer (EFT). These payments are processed using the automated fund transfer (AFT) system. Each business day, an electronic file of authorized payment information is sent by Banking and Cash Management to the Credit Union Central of British Columbia (CUCBC). The file is then processed by the CUCBC to distribute payments electronically to payees set up in the system, and an electronic file is sent daily to Banking and Cash Management to be used for verification and reconciliation. (See section F, below, for further details.)

In auditing this electronic payment process, we focused on the controls in place to address the risk that:

- processed payments are incomplete or inappropriately changed; and
- potential weaknesses in the service providers' (Credit Union Central of BC and Workplace Technology Services) processes and systems could cause malicious or accidental payment errors or delay EFT payments processing.

Key Findings

- A procedure manual for processing EFT payments exists, but some sections require updating.
- The access levels granted to some staff well exceed what is needed given their job roles. This has been addressed in Section A.
- Even though the AFT system restricts users from access to key payment information (payee name, bank account), users can exit from the system and – in some cases because of the access level granted – inappropriately gain direct access to the payment data files. This has been addressed in Section A.
- Duties are appropriately segregated between payment file creation (done by Corporate Accounting Services) and payment release to the CUCBC (done by Banking and Cash Management). However, there is no segregation of duties at

Banking and Cash Management between releasing the EFT payment file to the CUCBC and processing and releasing EFT rejected and recalled items. Compensating controls, such as notification to ministries of released, recalled and rejected EFT items help detect errors.

- Most payment files received by Banking and Cash Management auto-load to the AFT system through a scheduled process. However, some miss this process and are then manually loaded. There are system-based checks to ensure these payment files are not duplicated, however, there are none to ensure all files are processed.
- There are processes to ensure the initial payment information from ministries agrees to the summary data from the bank. However, we found instances where there was no direct evidence to support that these processes were performed.
- Policies and procedures for making program changes exist, but these are not consistently followed. Some weaknesses also exist in how changes to the AFT system and supporting applications are authorized and supported.
- Complaints from payees about payments are followed up and handled by ministries. This reduces the risk of payments that are accidently or fraudulently made for the wrong amount or to the wrong payee going undetected.
- The Financial Institutions Commission regulates credit unions and audits the CUCBC annually. An external audit firm also performs periodic reviews of the CUCBC's processes and systems. This provides government reasonable assurance about the quality of controls operating at the CUCBC.
- Assurance on processes and systems relating to the Workplace Technology Services operating environment is obtained through staff participation in pertinent cross-government committees.

Key Recommendations

- Banking and Cash Management should keep its EFT procedures manual current to ensure accurate guidance is provided to new employees and back-up staff.

- All instances of incompatible duties should be removed or additional monitoring activities added to manage the risk of accidental or intentional errors going undetected.
- Batch numbers should be traced to ensure all payment files are processed.
- There should be evidence to support control procedures have been performed. This would ensure that the initial payment information from ministries has been reconciled to the payment information received and processed by the bank.
- All program changes should be tracked and monitored to ensure they are approved and in compliance with change management policies.

D. Processing and printing cheques

Some cheque printing and distribution controls should be improved at BC Mail Plus.

BC Mail Plus, a branch of Procurement and Supply Services in the Ministry of Labour and Citizens' Services, provides mail preparation, handling, distribution and other services for all government ministries and a number of other government organizations. One of the important services it provides is the printing and mailing of government's manual cheques.

In auditing cheque printing and distribution, we focused on the controls in place to address the risks that:

- specially designed cheque stock is stolen to make fraudulent cheques;
- payment information is inappropriately altered during the printing process, resulting in cheques printed in error or fraudulently printed for personal gain; and
- printed cheques are distributed erroneously or lost during the distribution process.

We examined controls for managing blank cheque stock during the printing process, moving blank cheque stock from storage locations, and reconciling cheque stock. We also looked at how access to the MVS mainframe environment and the payment print files generated by Corporate Accounting Services are restricted; and

at the controls in place to ensure printed cheques were adequately managed during the distribution process.

Key Findings

- Duties relating to the sourcing of cheque supplies and to cheque printing are properly segregated.
- There is adequate accounting for, and security over, cheque stock supplies.
- Cheques are printed according to industry standards to reduce the possibility of fraudulent activities.
- Controls are generally adequate to ensure printed cheques are not distributed erroneously or lost during the distribution process.
- Void cheques and obsolete cheque stock are appropriately destroyed.
- Access to print and cheque storage areas at BC Mail Plus and the external facility is adequately restricted.
- Changes to the printing program appear to be appropriately authorized and documented.
- The number of cheques printed and the dollar value are reconciled to reports from Corporate Accounting Services.
- There are cases where access levels of print job operators exceed the operators' needs. This has been addressed under Section A.
- Several other control weaknesses exist, such as inadequate access logs and outdated procedures, which could potentially allow payment information to be inappropriately altered during the printing process.

Key Recommendations

- Several monitoring controls, such as access logs and staff lists, should be improved.
- Policies and procedures for staff should be updated, including those pertaining to cheque stock movements, testing procedures, reconciliations, and security measures.
- The cheque inventory tracking application should be password-protected and key cells locked to prevent accidental erasure and alteration.

E. Management of the status of payments

Controls should be strengthened over payment status management.

Although the dollar value of manual cheques processed by government has been declining in recent years because of the popularity of EFTs, there is still a considerable dollar value of cheques paid to suppliers ($3.2 billion in calendar year 2007 and $3.7 billion in calendar year 2006)[7].

Cheque management—for both automated and manual processes—involves tracking and accounting for all paid and outstanding cheques, coordinating stop payments with the bank, and requisitioning replacement cheques in a systematic manner so as to avoid duplicate payments. The cheque management system (CHQ) is used to manage this overall process (see Exhibit 2).

Management of EFT payments status involves tracking, recording and re-issuing or voiding payments that have been recalled by ministries or rejected by the bank. Recalls by ministries are managed by the automated fund transfer system (AFT).

In auditing payment status management, we focused on controls in place to address the risks that:

- paid cheque data is altered before it is loaded in the CHQ system or that it is incomplete;
- cheques are cancelled and fraudulently re-issued;
- stop payments and returned items are either not processed promptly or are processed without proper authorization;
- unclaimed cheques are cashed fraudulently;
- changes to the CHQ system are not authorized and documented;
- EFT payment recalls are either not processed in a timely manner or at all, resulting in potential losses to the government (because payments may not be recovered); and follow-up on rejected EFT payment transactions is inadequate and does not ensure errors are corrected and transactions are re-processed on a timely basis.

[7] Source – Bank Billing System report for the period January 1 to December 31, 2007, provided by Banking and Cash Management Branch.

Key Findings

- There are policies and procedures for: handling stop payments, replacements and cancellations; posting unclaimed cheques; processing errors reported by the bank and the ministries; and processing EFT recalls and returns. However, some policies and procedures require updating.
- A job processing schedule has been established to ensure that EFT recalls are transmitted to the bank on a timely basis.
- Government policy is not always followed by ministries for processing and re-issuing cancelled cheques. For example, some cheques that are stopped for cancellation are not returned to Provincial Treasury.
- Access granted to some staff is not appropriate for their job requirements. This has been addressed under Section A.
- Project lists that track changes to programs, and problem logs that record changes to data to address processing problems, are both manual; logs are not regularly reviewed. This provides minimal assurance that the logs are complete or accurate.
- The summary report of paid cheques (from the CUCBC), used to ensure the completeness of payments loaded into the cheque management system, is not always reviewed.
- There are processes for dealing with undeliverable and unclaimed cheques, but there is not an appropriate segregation between handling the returned cheques and recording them, creating an environment where error or fraud could potentially occur.
- Banking and Cash Management staff investigate all returned items and record them in a manual log and in the CHQ system, but no reviews are done by management on the daily returned cheque files.
- A confirmation for returned items transmitted is received the following business day from the bank, and used to verify the appropriate accounts have been credited the right amounts.
- There is not always evidence supporting comparison of the AFT recalls confirmation report with the email notifications received from ministries.
- There is no regular management review of replacement cheque activity in the CHQ system.

Key Recommendations

- Policies and procedures for managing the status of payments should be regularly reviewed and updated for new and back-up staff.
- Banking and Cash Management staff should communicate to ministries the importance of complying with policies and procedures for cancelling and re-issuing cheques, as outlined in government's financial policy manual.
- All program and data changes should be tracked and monitored to ensure they are approved and complying with policy.
- The summary report of paid cheque data should be regularly reviewed to ensure that the data was successfully loaded into the system.
- Roles and responsibilities should be reviewed by management with the aim of minimizing incompatible duties with respect to processing undeliverable and unclaimed cheques.
- Review of daily returned items should be performed regularly. This should be done by staff not involved in processing or authorizing returned items.
- There should be evidence supporting comparison of the automated funds transfer (AFT) recalls confirmation report with the email notifications received from ministries.
- Replacement cheque records should be regularly reviewed by management to ensure they are complete and no duplicate payments have occurred.

F. Reconciliation of payments to the general ledger

Controls should be strengthened over the processing environment for reconciling cheque and EFT payments to those processed and authorized by CAS.

The bank reconciliation process is one of the key controls to ensure that only authorized payments are cashed and that the cash balances in the general ledger are reconciled to the bank accounts.

Corporate Accounting Services is responsible for the bank reconciliation of various disbursement accounts: US dollar, general, government agents, medical services, and seniors' supplements.

Reconciliation information is generated from the bank reconciliation system (BRS)—based on input from the cheque management system, the corporate accounting system, and financial institutions relating to cheques issued, paid and outstanding from previous periods.

Reconciliations are performed daily and monthly. The daily reconciliation is performed every morning on each disbursement account, and involves electronic matching of cheques issued to cheques cashed. The sole purpose of this process is to give the Credit Union Central of British Columbia (CUCBC) timely feedback in case of fraud or errors. Monthly reconciliations are performed on each account and are executed on the sixth working day of the month after the general ledger is closed.

Our audit scope included the key processes in the bank reconciliation carried out by Corporate Accounting Services to ensure that all authorized payments have been processed accurately, completely and on a timely basis and that no other payments have been made. We therefore assessed controls related to the BRS that runs in government's MVS operating environment.

In auditing the reconciliation of payments, we focused on controls in place to address the risks that bank reconciliations are performed with incomplete or inaccurate data.

Specifically, we looked at the administration and maintenance of appropriate access to programs and data files that are used by the BRS; and at the reconciliation of cheque and EFT payments to those processed and authorized by the corporate accounting system.

Key Findings

- The bank reconciliation function is independent from authorization, initiation and cheque preparation operations. This is an appropriate segregation of function.
- Input files for the bank reconciliation are only from source systems such as CAS, CHQ, CHIPS and other ministry systems.
- Files interfaced by BRS are current versions, and the update process is routinely scheduled.
- There are adequate procedures over job scheduling to ensure current files are used in running bank reconciliation reports.

- The program logic for the daily matching of issued payments to cheques cashed is working as intended.
- The documented change management process at Corporate Accounting Services lacks specific details and direction on change controls for the MVS environment.
- Changes to programs are recorded in a manual log. This does not provide an adequate audit trail over the completeness or accuracy of program changes.
- Users with the ability to make changes to production programs and data are not appropriately segregated from the testing and development environments. This has been addressed under Section A.
- Access granted to some staff is not appropriate for their job requirements. This has been addressed under Section A.

Key Recommendations

- Specific reference should be made in the maintenance process manual to the change management processes needed for applications running in the MVS mainframe environment.
- To provide assurance on the completeness of the manual change log, high-level profiles protecting computer program files should be flagged so that when a change is made, the user is identified and logged for later review.

G. Back-up of program and payment files

Controls were adequate to ensure the timely back-up and recovery of program and payment files.

Important to any computing environment are processes to ensure the continuity of operations in the event of an unscheduled disruption[8]. Regularly making secondary copies of data and program files (back-ups) and storing them in a separate location, as well as having the ability to recover them if needed, helps to ensure this continuity.

[8] This section deals only with the recovery of payment data and programs, the following section deals with the larger issue of disaster recovery and business continuity.

In auditing back-up and recovery, we focused on controls in place in the MVS environment to address the risks that:

- payment processing is temporarily delayed because of inadequate plans, processes and testing; and
- once processing resumes, payment transactions are not complete or accurate.

To deal with such risks, policies and procedures should be in place to manage daily IT operations—including back-up procedures—and the files created as back-up must be tested to ensure that the system can be resumed in a timely manner.

Key Findings

- Back-ups of payment programs and data follow industry standards. For example:
  - daily incremental back-ups are done;
  - weekly data back-ups are done;
  - image copy tapes (complete database back-ups) are made; and
  - back-up tapes are secured with physical access controls and are stored in a location separate from the processing facilities.
- TELUS, under contract to operate and manage the MVS environment for government, uses an aggregate back-up and recovery service (ABARS). This service allows customers to back up and recover critical and unique applications. It also allows a point-in-time back-up of a collection of related data in a consistent manner. These back-ups are generally used for disaster recovery or to move applications across non-sharing systems.
- Tests are conducted annually by TELUS and Workplace Technology Services (WTS) to reconstruct the MVS operating environment from data, operating systems and programs held in off-site storage. These tests, in effect, also test the completeness of data in the off-site location and the instructions for systems recovery. Staff at Corporate Accounting Services, Banking and Cash Management and BC Mail Plus also participate in these annual exercises as part of their own testing of their disaster recovery plans (see section H below).

Key Recommendations

- None noted

H. Business continuity planning

Business continuity and disaster recovery plans and processes are reasonable, but a more coordinated approach is needed.

Backing up payment programs and data so they can be recovered and processing resumed after a temporary disruption to computing operations is one issue (as discussed in section G). A broader issue, discussed here, is that of having plans and processes to ensure that payment operations can continue in the event of a natural or human-caused disaster.

A well-designed and tested disaster recovery plan is usually a significant component of a business continuity plan. A disaster recovery plan requires business units to prioritize their critical processes according to their need for availability. To ensure these critical business processes are restored within an acceptable timeframe, IT recovery planning must be integrated with business unit continuity planning.

A risk analysis is also needed, to provide a structured approach for considering the damage from disaster events and the likelihood of their occurrence. Management's goal should be to strike a balance between the adverse effects of these risks and the cost of protective measures. In the case of Banking and Cash Management, for example, the following points should be considered:

- What is the likelihood that an event could occur that causes an interruption in processing cheque and EFT payments?
- How would such an interruption affect government's normal business processes if payments cannot be processed over an extended period?
- Based on those effects on normal business processes, what is management willing to spend in time and resources to ensure appropriate protective measures are in place?

The Risk Management Branch and Government Security Office in the Ministry of Finance and the Information Security Branch in the Ministry of Labour and Citizens' Services provide tools, resources and guidance to ministries in the development of their Business

Continuity Management programs. This guidance outlines the minimum requirements for business continuity plans.

In auditing business continuity planning, we focused on the risks that:

- payment processing and management functions are delayed for an unacceptable period of time because a disaster disrupts the processing environment; and
- no up-to-date plan or adequate processes are in place to allow resumption of payments and management functions needed for using alternate payment methods.

A destructive event could potentially interrupt government's Victoria-based payment operations in the: MVS or UNIX processing environments; BC Mail Plus facility; Corporate Accounting Services' office; or the facility housing the Banking and Cash Management office.

We expected that the risks associated with each of these occurrences would be assessed and that, in the event of a disruption, Corporate Accounting Services, BC Mail Plus, Banking and Cash Management, and Workplace Technology Services would have adequate plans to allow essential business operations to continue.

Key Findings

- Government policies are adequate to guide those involved in preparing continuity plans.
- Each of the four key business areas (Corporate Accounting Services, BC Mail Plus, Banking and Cash Management, and Workplace Technology Services) has a documented disaster recovery plan and business continuity plan. All plans have been updated within the last year, although the plan for Banking and Cash Management needs to be updated for the last recovery exercise in July 2007.
- Each business area is at a different stage of testing and monitoring the effectiveness of its plans.
- No plan is yet in place to ensure that all business continuity plans can work together. A Memorandum of Understanding (MOU) between Corporate Accounting Services, BC Mail Plus, and Banking and Cash Management includes a section that would see all three parties jointly developing and

maintaining a business continuity plan that would enable processing and printing of critical payments. This continuity plan is still being developed.

- The Ministry of Finance recently established an Alternative Payment Mechanism working group, tasked with developing alternate payment mechanisms in the event of a disaster.

Key Recommendations

- Banking and Cash Management Branch should update its business continuity plan promptly after each disaster exercise.
- Corporate Accounting Services should conduct an alternate site exercise.
- Corporate Accounting Services, Banking and Cash Management, and BC Mail Plus should jointly develop and maintain business continuity plans that will satisfy the minimum processing and printing requirements to enable critical payments to continue in the event of a disaster.

Appendix A: Glossary

Aggregate Back-up and Recovery Services (ABARS)

The Aggregate Back-up and Recovery System is a facility used to back-up and restore application related data sets as one group. *(Source: MVS user guide from the WTS website)*

Advanced Function Printing (AFP)

AFP is a printer driver for the high quality Xerox MICR (Magnetic Ink Character Recognition) printers at BC Mail Plus (BCMP). It is an IBM product and is customized for BCMP printing functionality.

Automated Fund Transfer or AFT System (AFT)

AFT is the application used by Banking and Cash Management (BCM) to process and release Electronic Fund Transfer (EFT) and Pre-Authorized Debit transaction files for ministries, agencies and Crown corporations. It consists of two modules:

1) Automated Fund Transfer System — processes and releases AFT payments, and
2) Payment Recall System — processes AFT payment recalls.

Banking and Cash Management Branch (BCM)

The Banking and Cash Management Branch at Provincial Treasury (Ministry of Finance) manages the Province's banking and financial arrangements and delivers a broad range of banking services. This includes cash management, bank payment processing, revenue consolidation and electronic banking services to ministries, Crown corporations and public sector agencies. *(Source: BCM website)*

Bank Reconciliation System (BRS)

Information for the bank reconciliation performed by Corporate Accounting Services is generated from the bank reconciliation system (BRS)—based on input from the cheque management system (CHQ), corporate accounting system (CAS) and financial institutions regarding cheques issued, cheques paid, and cheques outstanding from previous periods.

Corporate Accounting System (CAS) Oracle

This is the corporate financial system for the Province of British Columbia using the Oracle Financials application. It is a centralized, integrated off-the-shelf financial system that has been tailored to suit the requirements of provincial government ministries and agencies. *(Source: Corporate Accounting Services website and Introduction to CAS Oracle Financials user manual)*

CAS Generic Interface (CGI)

CGI is a mechanism that ministries and agencies can use to batch load their financial data into CAS Oracle. It enables Ministry Financial Information Systems (MFIS) and Ministry Program Financial Systems (MPFS), referred to as "feeder systems", to interface financial transactions into CAS Oracle. *(Source: Corporate Accounting Services website)*

Appendix A

Corporate Human Resource Information and Payroll System (CHIPS)

CHIPS is a corporate system of the Provincial government that assumes the responsibility of maintaining human resource information, tracking employee leave and processing payroll for government employees. Software currently being used is Peoplesoft 8.9.

Cheque Management System (CHQ)

CHQ is an application which tracks location and status of cheques—a database used to record cashed cheque information, stop payments and returned undeliverable/unclaimed cheques. It receives information from CUCBC and provides daily and monthly files of paid cheques to Corporate Accounting Services.

Credit Union Central of British Columbia (CUCBC)

CUCBC is the financial institution that holds the main disbursement accounts of the Province of British Columbia.

Electronic Fund Transfer (EFT)

An EFT process is a widely used technical solution deployed by corporations throughout the world to transmit payment instructions to financial institutions for payment of employees, companies and/or other entities. *(Source: ISACA website article "Preventing EFT Fraud" by John E. Humphries Jr., CISA, CISSP, GSEC Volume 4, 2003)*

Financial Institutions Commission (FICOM)

FICOM is a regulatory agency of the provincial Ministry of Finance and is responsible for administering 10 statutes that regulate the pension, financial services and real estate sectors in British Columbia. The primary focus of this regulation is to ensure that:

- Institutions and pension plans in these sectors remain solvent;
- Market conduct requirements for these sectors are respected;
- Unsuitable individuals do not participate in financial service markets; and
- Through the Credit Union Deposit Insurance Corporation (CUDIC), insure credit union deposits and non-equity shares up to the maximum defined by regulation ($100,000 per separate deposit) per credit union. *(Source: FICOM website)*

File Transfer Protocol (FTP)

FTP is a protocol used for exchanging files over the Internet. It is most commonly used to download a file from a server using the Internet or to upload a file to a server. *(Source: www.webopedia.com)*

Appendix A

Memorandum of Understanding (MOU)

A Memorandum of Understanding (MOU) is a written agreement, often used as the basis to discuss and agree upon mutual expectations. An MOU does not create legal or binding obligations, but is intended to provide a framework for a positive and co-operative working relationship between the parties. *(Source: Administrative Justice Office website)*

Multiple Virtual Storage (MVS)

MVS is the operating system for older IBM mainframes. It was first introduced in 1974 and continues to be used, though it has been largely superseded by IBM's newer operating system, OS/390. IBM's mainframe operating system is now called z/OS. *(Source: www.webopedia.com)*

Operating System (OS)

The operating system is the most important program that runs on a computer. Every general-purpose computer must have an operating system to run other programs. Operating systems perform basic tasks, such as recognizing input from the keyboard, sending output to the display screen, keeping track of files and directories on the disk, and controlling peripheral devices such as disk drives and printers. *(Source: www.webopedia.com)*

Resource Access Control Facility (RACF)

RACF or Resource Access Control Facility is an IBM developed software product employed to protect data and systems from accidental or intentional threats to confidentiality, integrity, and availability. This is achieved by controlling access to the individual resources found on the system. It provides complete auditing facilities to track and report on the activities of users and datasets. *(Source: Introduction to RACF users manual prepared by Common IT Services, now called WTS or Workplace Technology Services)*

SPAN/BC

SPAN/BC is a shared private data communications network for the Provincial Government that connects government offices throughout the province to a core (backbone) network and the Internet. It enables connectivity and electronic service delivery between the BC Government, the broader public sector, the business community and the citizens of the province. *(Source: SPAN/BC Overview)*

TELUS

The Province has comprehensive service agreement for MVS services with IBM.
IBM subcontracted the services to TES (TELUS Enterprise Solutions), now called "TELUS ITI" (TELUS Information Technology Infrastructure).

UNIX

UNIX is a popular multi-user, multi-tasking operating system developed at Bell Labs in the early 1970s. It was designed to be a small, flexible system used exclusively by programmers. *(Source: www.webopedia.com)*

Appendix A

Workplace Technology Services (WTS)

WTS provides IT infrastructure services for the BC government and the broader public sector. These include: data centre services, desktop support and service desks, voice and data networks, electronic messaging and directories, applications and service integration, and security/virus protection. *(Source: WTS website)*

Appendix B: Office of the Auditor General Reports Issued During Fiscal 2008/2009

Report 1 – April 2008

An Audit of Joint Solution Procurement and the Revenue Management Project

Report 2 – April 2008

Strengthening Accountability in British Columbia: Trends and Opportunities in Performance Reporting

Report 3 – May 2008

Management of Aboriginal Child Protection Services

Report 4 – May 2008

Managing Government's Payment Processing

This report and others are available on our website at: http://www.bcauditor.com